FPNの提案とその実現

名城大学理工学部

キーワード：

ユビキタスネットワーク

ネットワークセキュリティ

ＵＲＬ　http://www-is.meijo-u.ac.jp/~watanabe/

研究のねらい

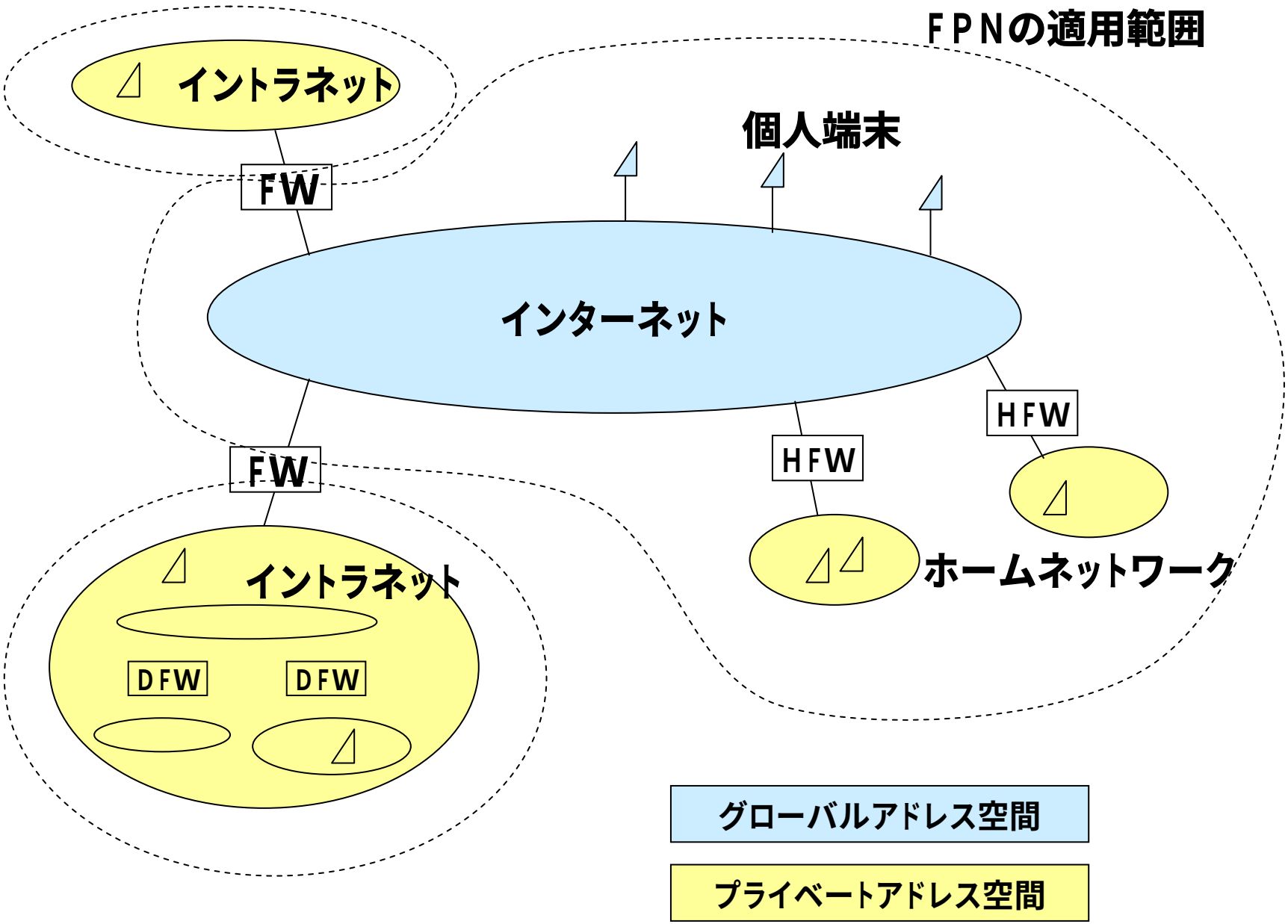
自由に動ける

安全に使える

研究の名称

FPN (Flexible Private Network)

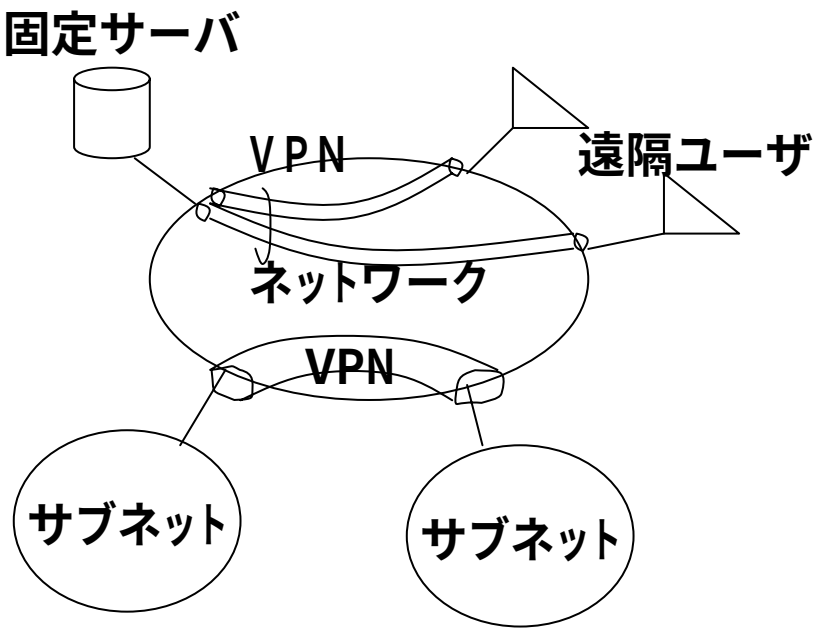
柔軟性とセキュリティを兼ね備えたグルーピング通信を可能とするネットワークシステム


ＦＰＮの適用範囲
イントラネット
個人端末
ＦＷ
インターネット
ＨＦＷ
ＨＦＷ
ＦＷ
イントラネット
ＤＦＷ
ＤＦＷ
ホームネットワーク
グローバルアドレス空間
プライベートアドレス空間

VPN (Virtual Private Network)

既存技術

ネットワークのインフラを共有する手段として有効



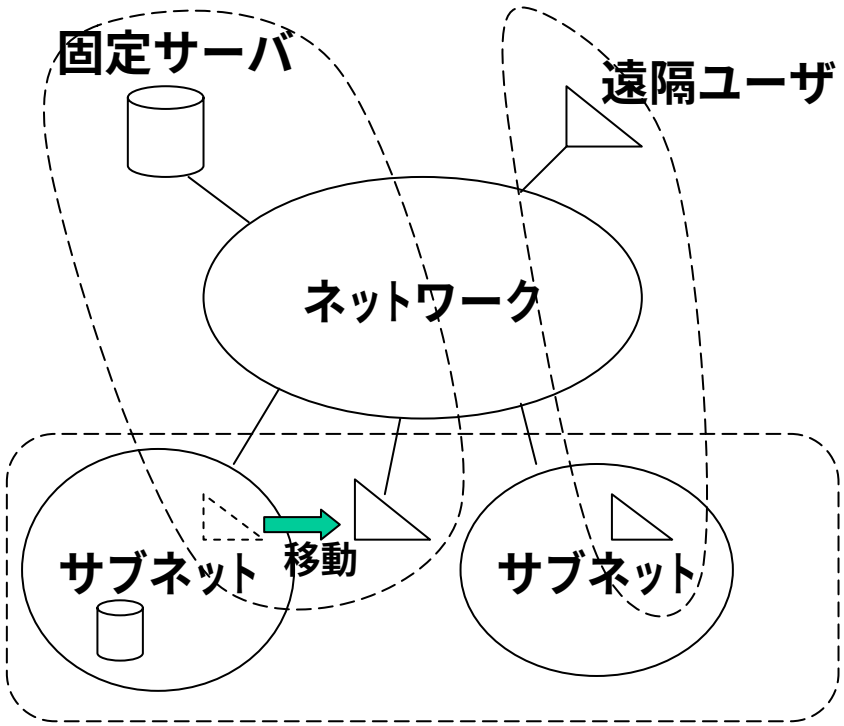
VPNの課題

・サブネットは固定、サーバは固定

・ネットワークは平坦

提案技術

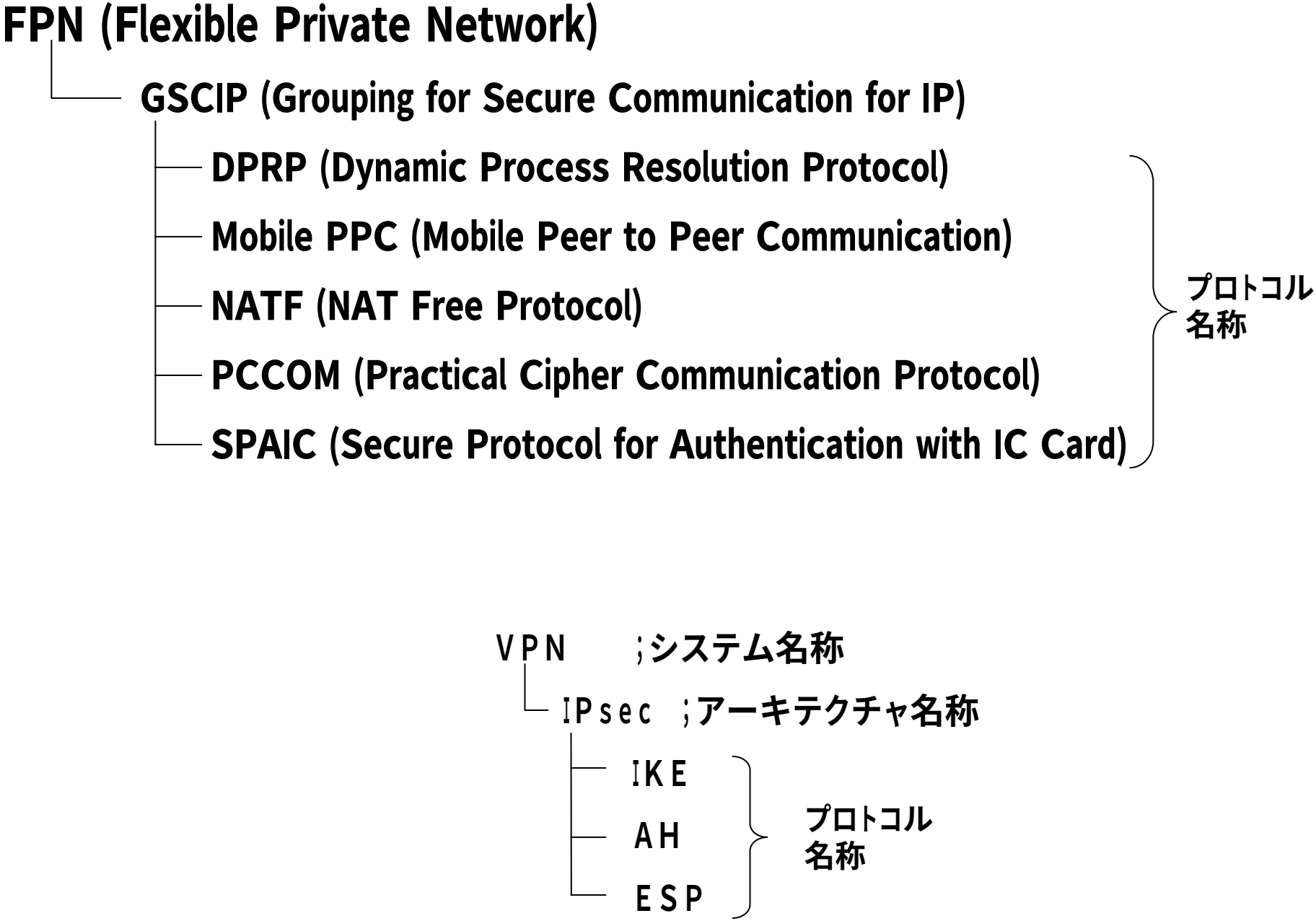
FPN (Flexible Private Network)



FPNの特徴

・すべてのホストが動くことを想定

・ネットワークの多段構成に対応


FPN (Flexible Private Network)
GSCIP (Grouping for Secure Communication for IP)
DPRP (Dynamic Process Resolution Protocol)
Mobile PPC (Mobile Peer to Peer Communication)
NATF (NAT Free Protocol)
PCCOM (Practical Cipher Communication Protocol)
SPAIC (Secure Protocol for Authentication with IC Card)
プロトコル名称
VPN ;システム名称
IPsec ;アーキテクチャ名称
IKE
AH
ESP
プロトコル名称

ＧＳＣＩＰ（ジースキップ）の機能

共通暗号鍵を用いた通信グループ定義

共通暗号鍵と通信グループを１対１に対応づけ

動作処理情報の自動生成（ＤＰＲＰ）

システム構成に応じて動作内容を自動的に変える機能
ネットワーク構成の学習。多段ネットワークへの対応

h

自由な移動通信（Ｍｏｂｉｌｅ　ＰＰＣ）

場所を移動しても通信を継続できる機能（通信開始時，通信中を含む）
エンドエンドで実現

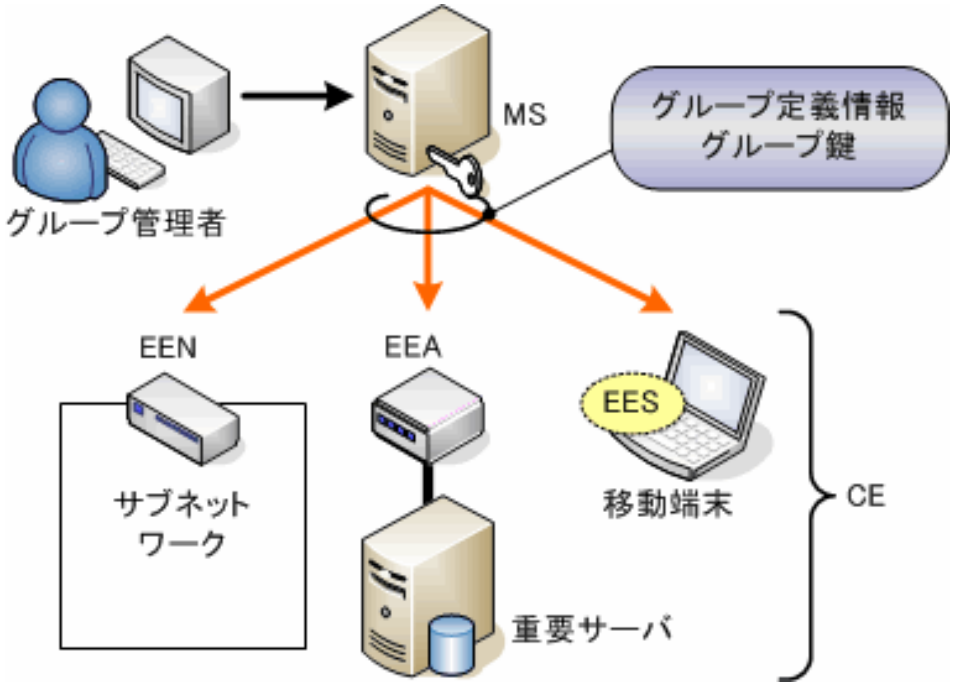
h

異なるアドレス空間を跨る移動通信（ＮＡＴＦ）

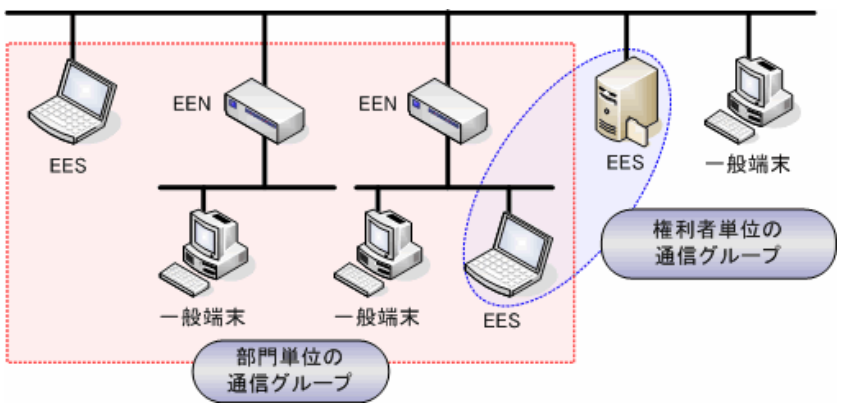
グローバルアドレス/プライベートアドレスの違いを意識しなくてよい。プライベートアドレスの管理が不要。

GSCIPの基本；共通暗号鍵を用いた通信グループの定義

提案技術

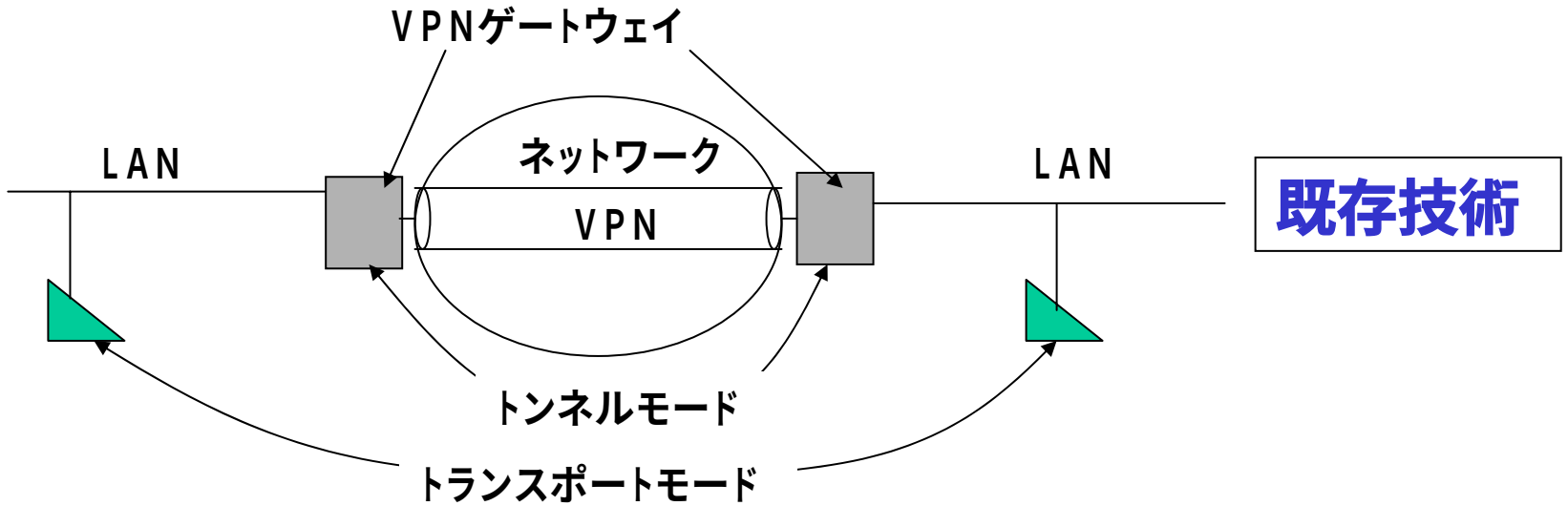


通信グループと共通暗号鍵を1対1に対応づける

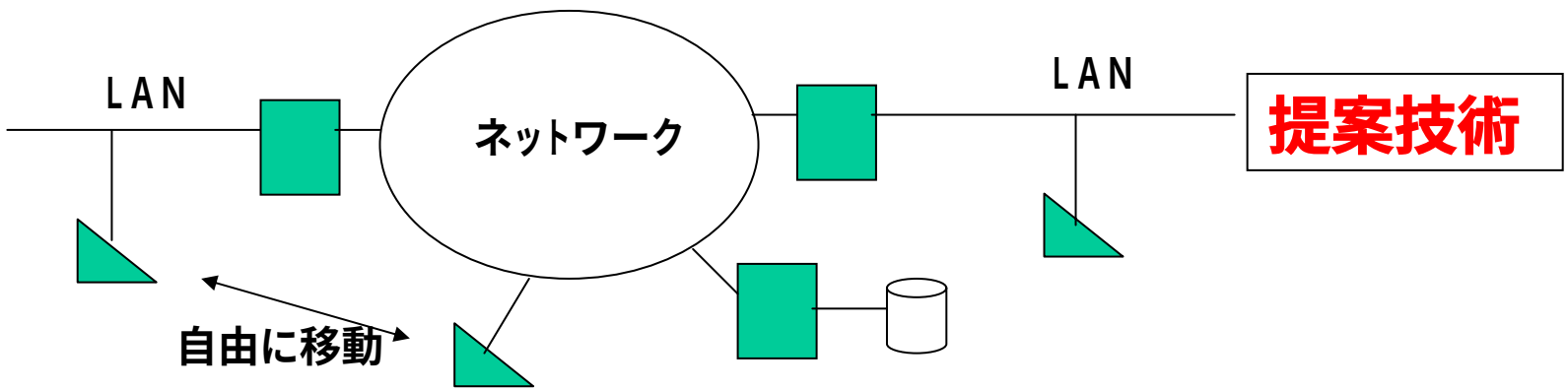


多段構成ネットワークでも同様に定義する

IPsecはトンネルモードとトランスポートモードに互換性がない→多段構成に柔軟に対応できない



GSCIPはすべての暗号装置が対等→多段構成に対応可能

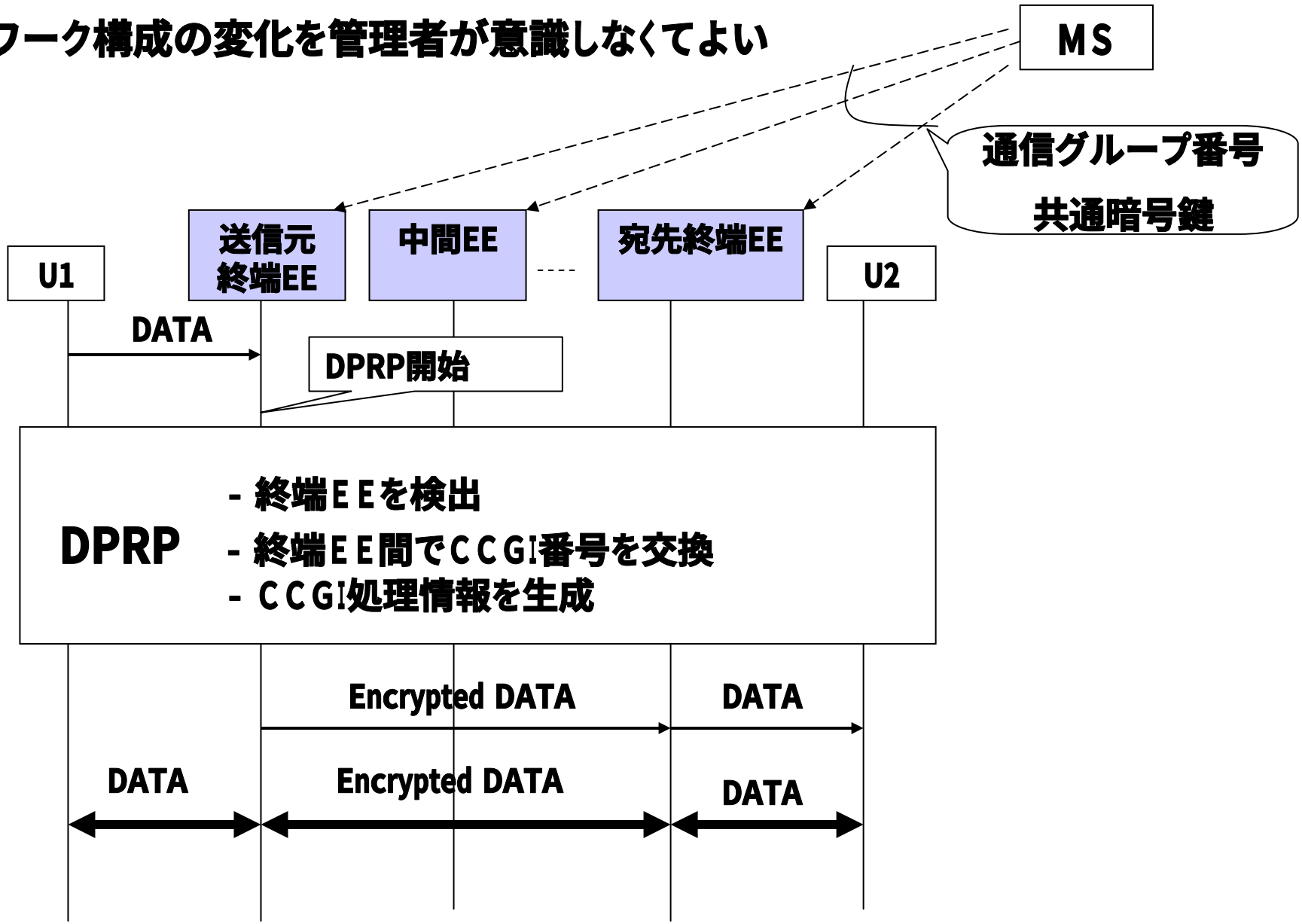


ＤＰＲＰ (Dynamic Process Resolution Protocol)

提案技術

ネットワーク構成を学習するプロトコル

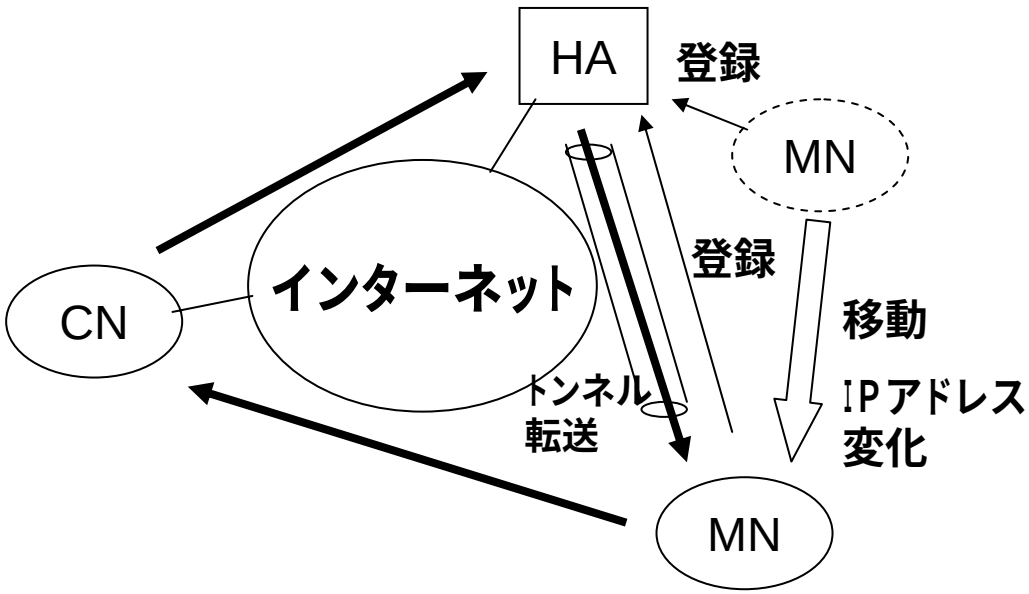
ネットワーク構成の変化を管理者が意識しなくてよい



Mobile IP

既存技術

通信中に移動しても通信を継続できる技術



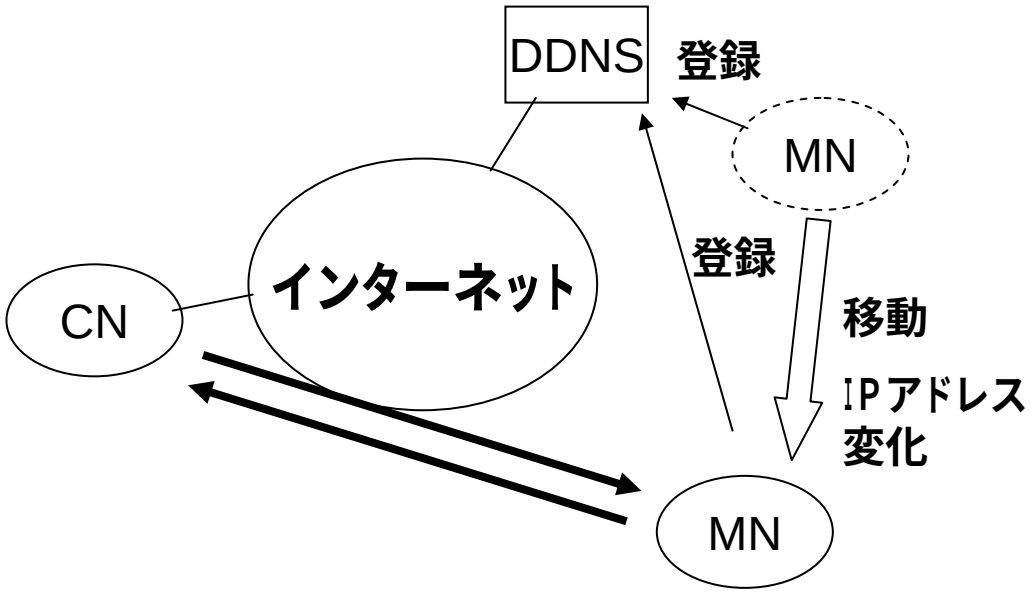
モバイルIPの課題

- **通信経路が三角経路となる**
- **HAとMN間はトンネル転送となる**
- **特殊な装置（HA）が必要となる**

→ Mobile PPC

Mobile PPC (Mobile Peer to Peer Communication)

提案技術



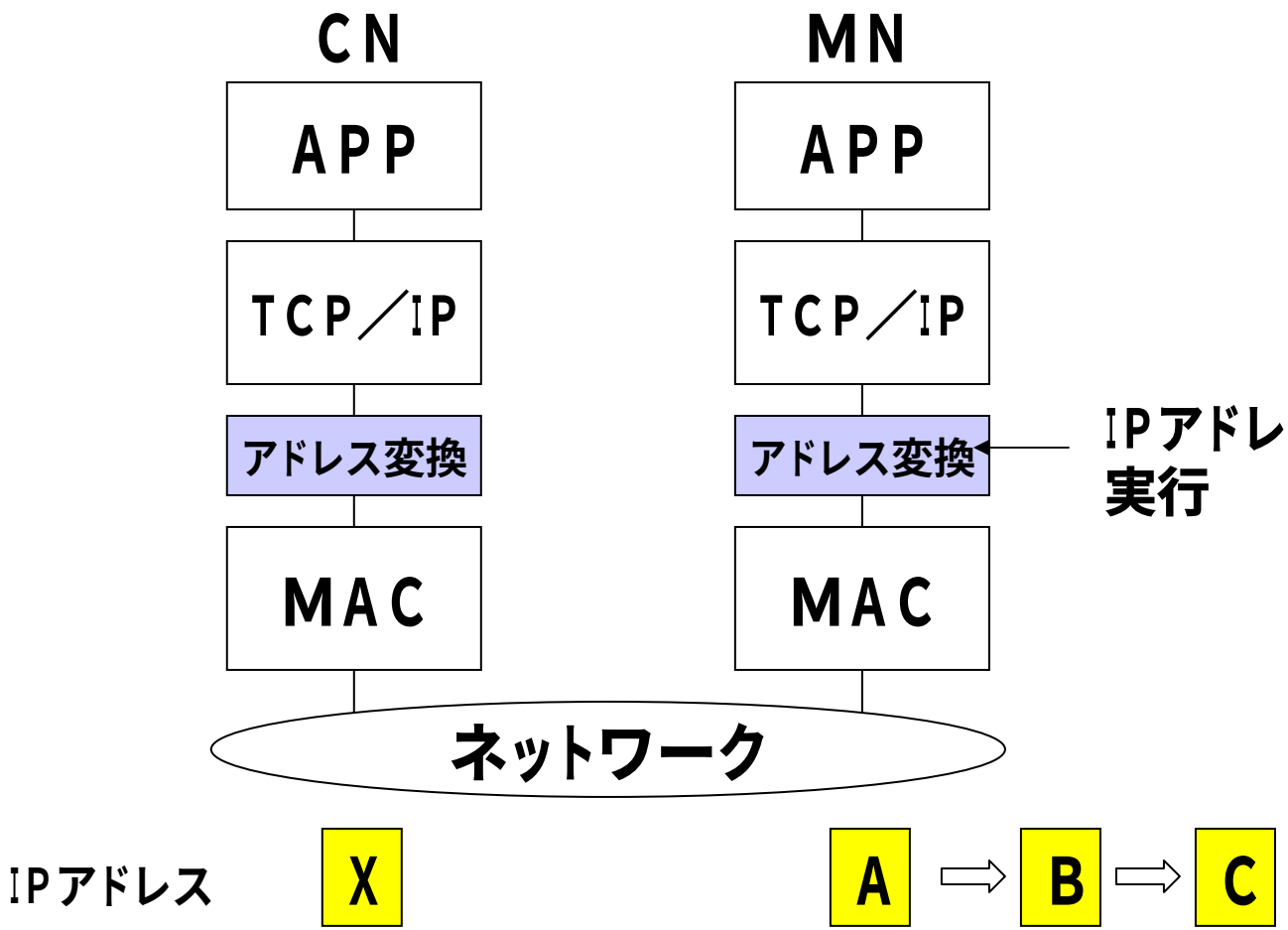
初期IPアドレスの解決にはＤＤＮＳ (Dynamic DNS)を使う。

アドレスの変更は拡張ＤＰＲＰを使用し、特別な装置を必要としない。

IPアドレスの変更はエンドエンドで通知する。アプリケーションはIPアドレスの変化に気付かない。

Mobile PPC (つづき)

提案技術



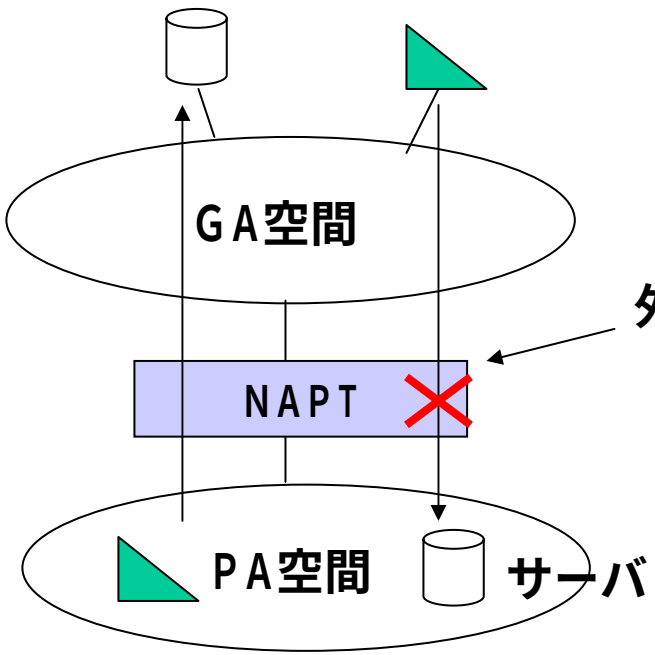
TCP／IPとMACの間でアドレス変換を実行することによりアプリケーションはIPアドレスが変化したことに気づかないようにすることができる。

FreeBSDに実装して確認済み。Windowsにも実装可能。

NAPT（IPマスカレード）

既存技術

NAPTがIPアドレス変換を行うことによりプライベートアドレス（PA）空間からグローバルアドレス（GA）空間のサーバへのアクセスが可能となる



NAPTの課題

・GA空間からPA空間のサーバへのアクセスができない。

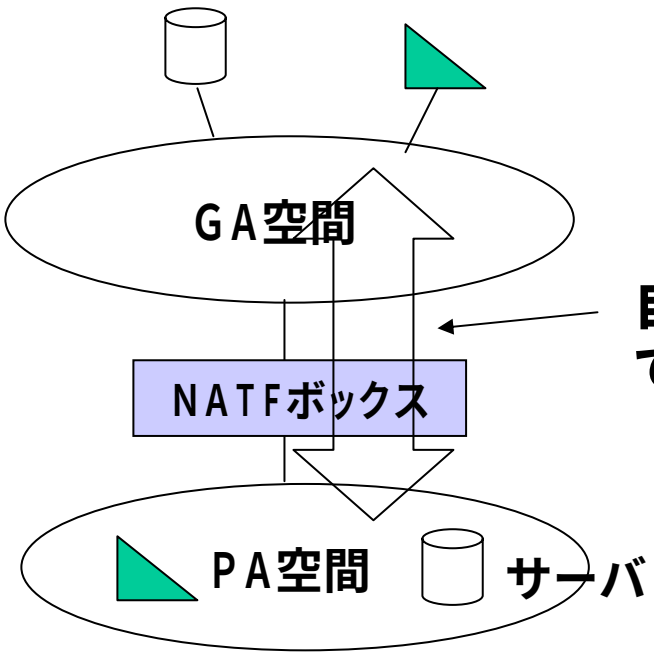
NATF

ＮＡＴＦ (NAT Free Protocol)

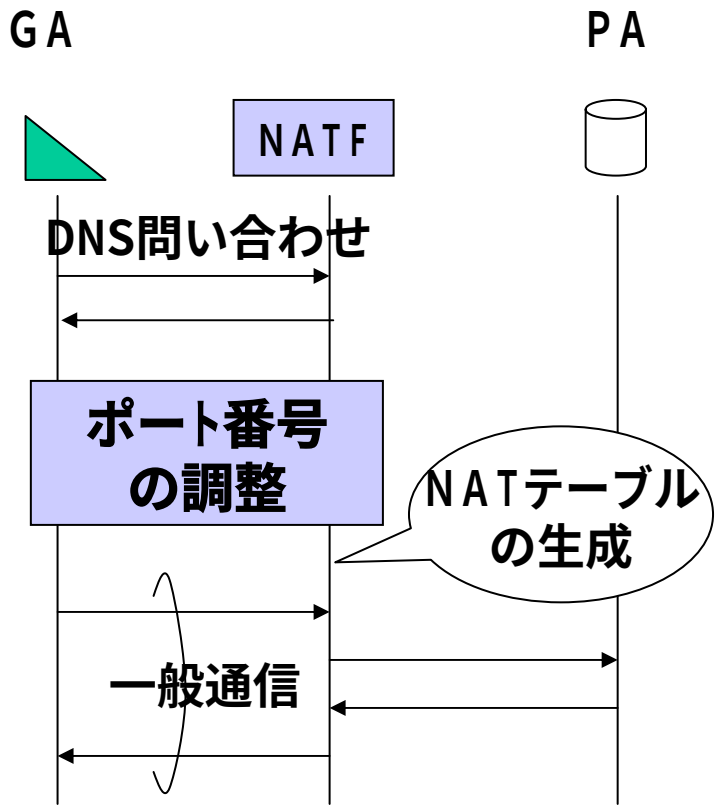
提案技術

ＧＡ空間の端末とＰＡ空間の端末が自由に通信できる。

ＧＡ端末とＮＡＴＦ　ＢＯＸがポート番号のネゴシェーションを行う。



自由に通信できる

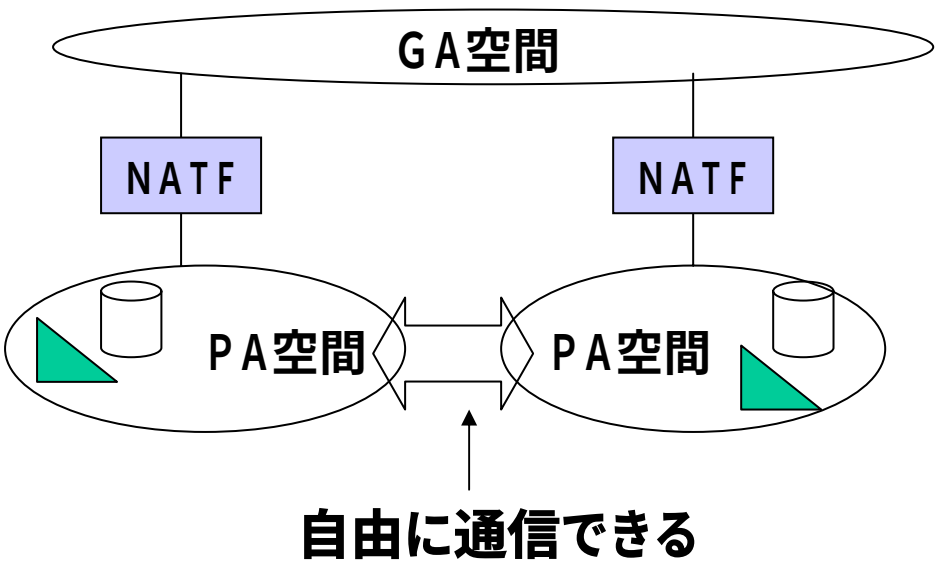


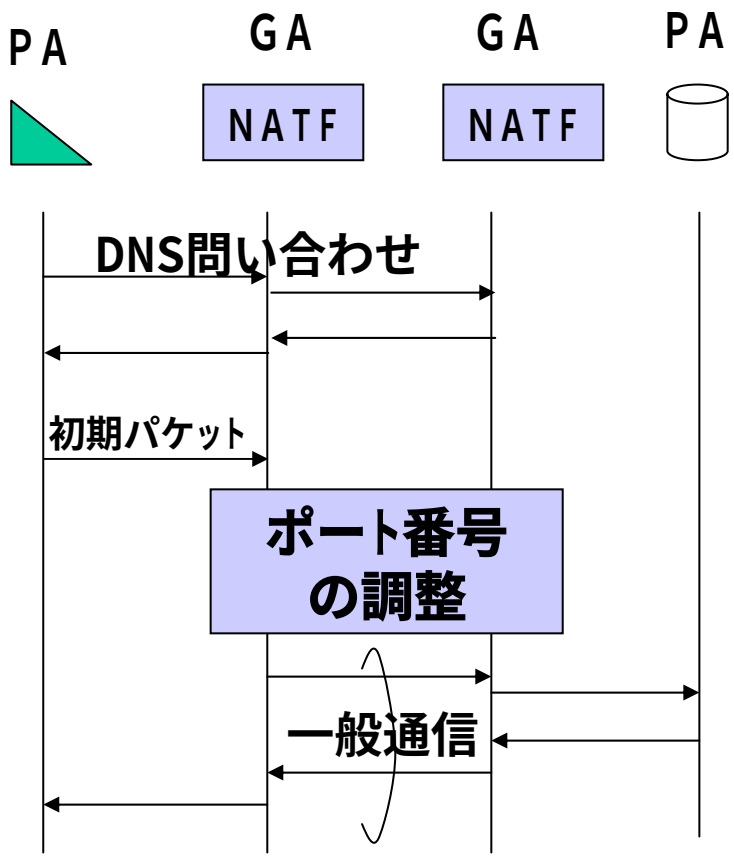
CIPA (Communication between terminals in Independent Private Address area)

提案技術

GA空間を介して異なるPA空間の端末どうしが自由に通信できる。

NATF　BOXどうしがポート番号のネゴシェーションを行う。

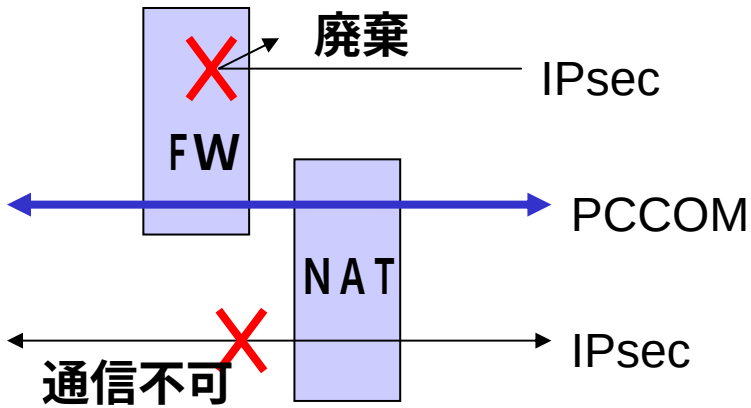




提案技術

PCCOM (Practical Cipher Communication)

ファイアウォール（FW）／NATを通過できる高スループット暗号通信プロトコル



・TCP／IPのパケットフォーマットは変えない　→高スループット

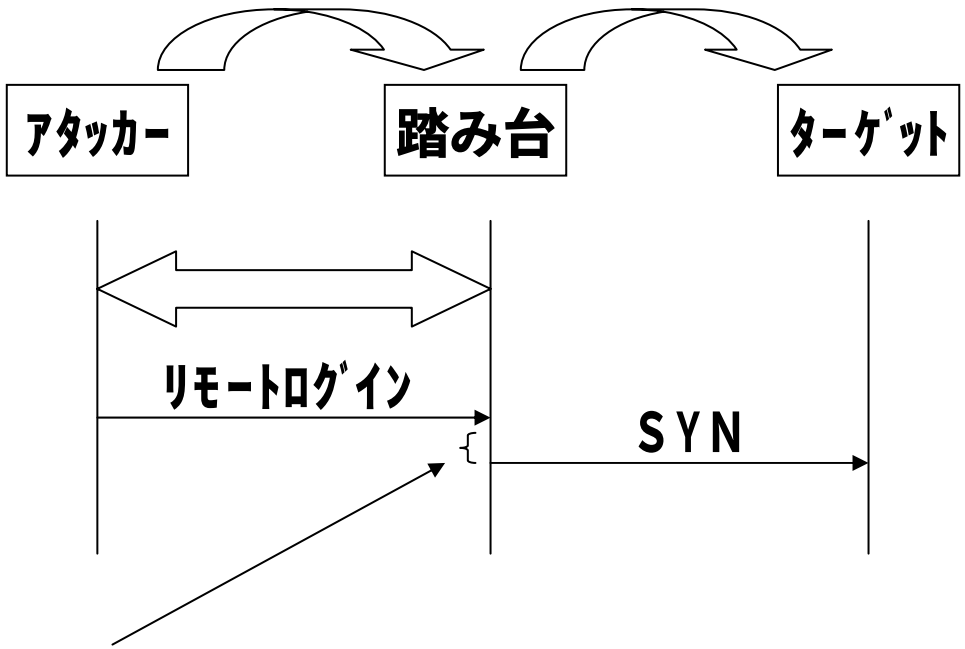
・IPアドレス、ポート番号は暗号化範囲からはずす　→FW／NATを通過できる

・パケット全体の完全性を保証する　→必要最低限のセキュリティを保持

提案技術

渡り歩きの検出

踏み台攻撃が発生していることをネットワーク上で検出する



踏み台ホストにおいて、リモートログインパケットを受信直後にターゲットへのＳＹＮパケットが送信されることに着目する

⇒　渡り歩きが検出できる！